SECTION IV. SECURITY INSPECTIONS

Part 1. INSPECTIONS

4-1oo Application. This part sets forth the purpose and establishes the procedures and schedule for the conduct of industrial security inspections.

4-101 Purpose. Security inspections shall be conducted for all cleared contractor facilities having access to classified information to ensure compliance with the requirements of the DoD Industrial Security Program. Such inspections shall ensure that procedures, methods, and physical safeguards employed by contractors are adequate for the protection of classified information entrusted to them. In addition, the Inspection shall serve as a method " for providing recommendations and suggestions to improve security practices at. the facility.

4-102 Reciprocal Use of DOE and DoD Security Inspection Programs. Existing security inspection agreements between CSO's and DOE activities, whereby CSO's perform inspections of DOE classified contracts at DoD-cleared contractor facilities or the DOE agrees to perform inspections of DoD contracts which may or may not involve RESTRICTED DATA at DOE facilities, will continue to be honored. However, such agreements should. be reviewed and updated as necessary to conform with the "general policy outlined in this paragraph. Copies of revised and new agreements entered into subsequent to the receipt of this regulation, shall be furnished the Director, DIS, ATTN: Deputy Director (Industrial Security).

a. A DoD CSO may, on receipt of a request from a DOE activity, enter into a written agreement to assume security inspection responsibility for a DOE classified contract being performed at a DoD cleared contractor's facility. The requesting DOE activity shall be responsible for notifying the contractor that the provisions of the ISM 1/ will apply to the DOE contract and that the security inspections will be performed by the contractor's present. DoD CSO. The DoD CSO will be responsible for:

(1) initially notifying the DOE requesting activity of the contractor's FCL and safeguarding ability, and the mailing address to which DOE classified material should be addressed;

(2) subsequently notifying the DOE requesting activity of any contemplated termination or revocation of the contractor's FCL, inability to safeguard the DOE classified information, or change in mailing address;

(3) ensuring that the DOE interests are covered during recurring inspections -- normally, copies of the DD Form 696 shall not be furnished the interested DOE activity; however, if requested upon initial award of a DOE contract or whenever an unsatisfactory security rating is assigned, a copy of the DD Form 696 shall be furnished; and

---

1/ If there are any exceptions, both the contractor and the DoD CSO shall be advised in writing.

(4) advising the interested DOE activity of any serious security deficiencies encountered or any case involving loss, compromise, or suspected compromise of classified information pertaining to the DOE contract. Such advice may be in the form of a copy of the letter to management, a copy of the investigative report of loss, compromise, or suspected compromise, or a synopsis of the overall status of security in the facility, including those deficiencies that specifically affect the DOE contracts.

b. A DoD CSO may enter into a written agreement with a DOE activity to perform certain DoD security cognizance actions when a DoD contract is being performed at a DOE cleared contractor's facility. In such cases, the security actions and responsibilities of the DOE activity and the DoD CSO shall be included in the DOE/DoD Agreement.

(1) The DOE activity shall be responsible for the following.

(a) Notify the CSO of any contemplated termination of DOE interest at the contractor's facility, or inability of the contractor to safeguard the DoD classified information, or any changed condition that would affect the contractor's DoD FCL (see paragraph 2-118).

(b) Assure that the DoD interests outlined in the written agreement are covered during security inspections. Normally, copies of the DOE inspection report shall not be furnished the DoD CSO. However, if requested on initial award of a DoD contract or whenever an unsatisfactory security rating is assigned, a copy of the DOE inspection report shall be furnished.

(c) Advise the DoD CSO of any serious security deficiencies encountered or any case involving loss, compromise, or suspected compromise of classified information pertaining to the DoD contract. Such advice may be in any appropriate form or format (see paragraph a(4) above).

(2) The DoD CSO shall be responsible for the following.

(a) Process and issue a DoD FCL in the normal manner to enable the contractor to bid on other classified DoD contracts.

(b) Advise the DOE activity of those paragraphs in the ISM that are either in addition to or different from DOE requirements and which should be covered by the DOE activity during inspection. For example, ensure that the contractor complies with sections V and VI and paragraphs 5, 6, 7, 10, 14, and 17, ISM 2/. Except as indicated, the DOE security requirements apply.

(c) As appropriate, arrange with DISCO to process personnel actions for individuals requiring a PCL in connection with the FCL and issuance

---

2/ The paragraphs of the ISM in the examples apply in all cases. However, based on the specific case at hand; there could be additional paragraphs of the ISM which should be delineated.

of a DoD LOC. In addition, personnel requiring access to DoD TOP SECRET information shall be cleared. by DISCO and issued a DoD LOC.However,accessto DoD SECRET information may be granted within the facility on a strict need-to-know basis without being issued a DoD LOC, provided the employee has a "Q" clearance. If the employee does not have a "Q" clearance or requires access outside the facility (for example, on visits), he or she shall be cleared by DISCO and issued a DoD LOC. Access to CONFIDENTIAL information may be granted based upon a contractor's CONFIDENTIAL clearance except as noted in paragraph 24, ISM.

(d) Notify the contractor in writing of the agreement reached with the DOE activity and also advise the contractor of his or her security responsibilities with specific emphasis on those items included in the DOE/DoD agreement in accordance with the two preceding paragraphs.

(e) Maintain liaison with the DOE activity immediately prior to and subsequent to the award of a DoD contract and upon completion or termination of the DoD contract to assure that all DoD requirements are complied with by the UA and the contractor.

4-103 Schedule. An initial inspection, in addition to the visit required by paragraph 1-110C or, 1-111b, shall be completed within 20 days from the time the CSO receives notice that the facility has classified material in its possession, but in any event, within 2 months from the date of the FCL. Initial" inspection of a COMSEC account shall be made jointly with a representative of the COR. Inspections of contractor facilities shall be conducted in accordance with the schedule indicated below.- This schedule does not preclude conducting inspections on an unannounced basis or at more frequent intervals wherever conditions at facilities dictate or when otherwise warranted. As an example, serious deficiencies encountered in a facility's security program would indicate a need for increased inspection effort. When an unannounced inspection is conducted, some of the administrative data normally furnished by the contractor, and entered on the DD Form 696, may not be 'available. In such cases, the information may be omitted from the DD Form 696, but shall be included at the time of the next announced inspection. In instances in which the contractor reports to the CSO the establishment of or any change in the location of a closed or restricted area within the facility, the CSO shall determine if it is necessary to make an inspection prior to the next regular inspection. Such determination should be baaed on the CSO's previous experience and knowledge of the contractor's operation plus an evaluation as to the contractor's past dependability in safeguarding classified material while an area is being established: "In these instances where parent and subsidiary facilities have entered into approved formal agreement as provided for in paragraph 72c, ISM, both facilities shall be inspected simultaneously.

a. The inspection schedule shall be based upon the highest level of classified material possessed at the facility since the preceding inspection except as otherwise provided below.

b. Inspection Schedule.

(1) Level of Possession	Frequency
TOP SECRET	6 months
SECRET	6 months
CONFIDENTIAL	9 months

(2) All other facilities, except as noted below . 9 months

c. It is the responsibility of the Deputy Director (Industrial Security), HQ DIS to ensure that specific unannounced inspection standards and criteria be developed and that they be uniformly applied throughout each Cso. Unannounced Inspections shall be approved in advance by the cognizant Director of Industrial Security, his or her designee, or higher authority.

d. The inspection schedule for facilities which are candidates for administrative termination may be lengthened or shortened to accommodate the requirements of paragraph 2-119.

e. HOF's of commercial carriers and their terminals listed on the DIS Form 1150 which have been granted a FCL will be inspected every 6 months.

f. Graphic arts facilities will be inspected every 6 months.

g. CSO's will arrange to inspect periodically selected uncleared locations where cleared personnel are employed or physically located to verify the continuing adequacy of the alternative procedure to annual visits provided for in paragraph 73, ISM.

h. CSO's will, in conjunction with performing regularly scheduled industrial security inspections, "conduct OPSEC inspections to assess contractor compliance with UA imposed OPSEC requirements. Section X provides further guidance on these type inspections.

4-104 Notification of Inspection.

a. Prior to visiting a facility for the purpose of a recurring inspection, the facility shall be notified approximately 10 days in advance of the impending visit. This, in addition to being a common courtesy, affords the FSO an opportunity to prepare for the inspection. For instance, he or she has to verify that representatives of management will be available for discussions and for the post inspection critique, and that other key personnel such as the document control supervisor, contract administrator, and reproduction supervisor will be available for interview. Finally, the contractor needs sufficient time to prepare a list of classified contracts on which the facility is currently performing.

b. Prior to effecting an inspection at a contractor facility, the inspector shall accomplish the following.

(1) Review the previous DD Form 696, related correspondence, and any subsequent reports. Deficiencies recorded on the preceding DD Form 696 report should be noted and the extent of corrective action checked during inspection. Failure to correct the deficiencies during the interval between the inspections shall be discussed with management to determine its attitude toward its security program.

(2) Review the list of current classified contracts, the DD Forms 254, and related forms. This review will, in addition to indicating the highest classification of material that should be in the facility, reveal

whether or not classified material in the form of hardware or equipment is to be produced. If so, the inspector should be alerted to the fact that there would, or should be, controlled areas to be inspected at the facility. Note the dates shown on the DD Form 254 for evidence of failure on the part of the contracting activity to conduct required biennial reviews. In each instance the DD Form 254 should be reviewed carefully prior to the inspection.

(3) Take note of any special access requirements or other additional security requirements for particular contracts.

(4) Review any reports of recent security violations. Reports submitted by the facility under paragraphs 6a(2) and (3), ISM, should be screened. An excessive number of such reports, particularly if they are similar in nature, would indicate a laxity In the facility's document control system, educational program, or both. Absence of such reports is also worth noting. If the loss of documents or other indications of compromise are detected during the inspection (when it is established that the facility has prior knowledge of these conditions), this would be an indication of failure to comply with the ISM reporting requirements.

(5) Review the facility's SPP to ensure that it provides a complete set of adequate procedures which specify what is to be done, how it is to be done, who is to do it, and who is to supervise it. If there are omissions in the SPP, or if the SPP has not been set forth in sufficient detail, it is likely that deficiencies will be discovered during the inspection in the same areas in which the procedures are silent or covered in general terms. Note also if the last revision to the ISM has been incorporated into the procedure.

If plant representatives or their designees are at the facility (including DCASR plant representative), they shall be alerted to the forthcoming inspection and visited as soon as possible after arriving at the facility. In addition, every effort shall be made to brief the plant representatives or their designees of the inspection results in advance of the briefing to be given to management. 'If the plant representatives or designees are not available, they will be apprised of the inspection results as soon as possible, after conclusion of the inspection, by copies of correspondence. An invitation shall also be extended to the plant representatives or their designees to attend the management critique and they shall be placed on distribution for copies of correspondence subsequently sent to management' relative to the inspection.

d. In those instances where the CSO elects to perform an inspection on an unannounced basis as provided for in paragraph 4-103, the notification provisions outlined above will not apply.

4-105 Use of Industrial Security Inspection Report (DD Form 696). This form is designed to focus attention on the security requirements established in the ISM and DoD 5220.22-S-1 (reference (q)), as well as to serve as a guide for the conduct of security inspections. When filled in, the original of the form shall be maintained by the CSO in the facility file folder in order to have available the latest information for the evaluation of the current security status of the facility. The completed forms are not routinely distributed to UA's or the contracting officers having procurement

responsibilities at the facility; however, the CSO shall, on request, furnish advice as to the latest security conditions of the facility. A DD Form 696 is generally useful to the UA's only when the facility has been evaluated as "unsatisfactory." In such cases the CSO will automatically furnish a copy of the DD Form 696 to every contracting activity concerned, under the provisions of paragraph 4-201.

4-105.1 TEMPEST Countermeasures.

a. DoD policy requires contractors to take TEMPEST countermeasures only if such special security requirements are specifically incorporated into th-e contract by -the UA whose classified information is processed. A copy of these special security requirements shall be furnished the CSO by the UA.

b. Contracting officers shall ensure that potential compromising situations related to the performance of classified contracts are identified and evaluated, and, where appropriate, include in such contracts requirements for the security countermeasures necessary to ensure compliance with national policies for the control of compromising emanations. When such contract requirements are established, the CSO shall be advised.

c. Tlie CSO may obtain technical assistance from the contracting officer or his or her designated representative when necessary in connection with the inspection of a contractor's facility for compliance with TEMPEST countermeasure provisions of the contract.

d. In those instances where the UA has not incorporated special security requirements as TEMPEST countermeasures in the contract, and the CSO believes such measures are warranted, the CSO should bring the matter to the attention of the appropriate contracting officer. If more than one UA utilizes the equipment, the issue should be discussed with all contracting officers whose classified information is being processed. Factors to be considered by the CSO will be: (i) the type of equipment or component involved, (ii) the physical environment in which the component is located, (iii) the sensitivity of the classified information, and (iv) the frequency, volume, and duration of classified information processing.

e. Contracting officers should direct any questions concerning TEMPEST policy or countermeasures to the following activities.

Director
National Security Agency
ATTN: S6
Fort George G. Meade, MD 20755

Commander
U.S. Army Intelligence & Security Command
ATTN : IAOPS-OP-P
Arlington Hall Station
Arlington, VA 22212

U.S. Air Force Cryptologic Support Center
ATTN : EPV
San Antonio, TX 78243

Commander
Naval Security" Group Command
ATTN : G-65
3801 Nebraska Ave., NW . "
Washington, D. C. 20390

4-106 Use of the DIS Form 1148. This is a multipurpose form designed to focus attention on the security requirements established for commercial carriers.

a. The purpose of part I is to develop sufficient facts and to ensure submission of necessary documents to permit an administrative determination to grant or deny a security clearance to a HOP and terminals listed on the DIS Form 1150 of a commercial carrier. It is also the basis for a CSO of the HOF of a carrier to determine if the overall carrier organization should be granted authority to transport SECRET material. In addition, part I is utilized to develop information concerning changed conditions, such as a change of address or reorganization. Part I is also to be used by the CSO in determining whether the HOP of the commercial carrier is subject to FOCI factors. The information in part I and attachments thereto is used as an aid to investigation in such cases. Whenever part I is used, the original of the form with all attachments will be forwarded to DISCO. The CSO will retain a copy In its facility file f elders.

b. The purpose of part 11, when used in conjunction with the applicable inspection check list, is to provide for uniform and comprehensive security inspections of cleared facilities of commercial carriers to determine compliance with the requirements of reference (b), as well as the ISM, as appropriate. When part II is used, the CSO will retain a copy in appropriate facility file folders in order to-have available the latest information pertaining to the security status of the facility inspected. In addition, the CSO of the HOF will be furnished and will retain copies of reports and correspondence pertaining to violations or major deficiencies (including unsatisfactory reports) for all of the carrier's terminals in order to have available the latest information pertaining to the overall security status of the carrier's organization (system). As necessary, the CSO of the HOF will assist other CSO's over terminals in obtaining satisfactory corrective action from top management officials of the HOF. The information in part II is not intended for routine distribution; however, the CSO shall, on request, furnish advice as to the security status of the commercial carrier.

c. Instructions governing the use of this form are contained in paragraph 9-206.1.

4-107 COMSEC Inspections.

The purpose of the inspection of a COMSEC account is to determine whether * contractors are complying with the requirements of reference (q) and such * additional security requirements as. may be provided for by the individual * contracts for the safeguarding of COMSEC information. The inspection 1s * designed to obtain an overall security evaluation of the facility's pro- * tection of COMSEC information and the current security status of COMSEC * information in the facility. Following each COMSEC inspection, the CSO * shall provide a report of the inspection to the appropriate COR. *

4-108 **Formal Notification.**

a. The contractor shall be notified in writing of the results of the inspection. The letter shall be addressed to management and not to the FSO. A copy of this letter may be sent to the FSO. While a basic format for these letters is acceptable, each should be a typed letter rather than a printed form. The notification shall identify all significant security deficiencies noted during the inspection with specific reference to the appropriate paragraphs of the ISM. The facility shall be given a specific date by which all deficiencies cited shall be corrected, and requested to notify the CSO when the corrections have been accomplished.

b. Depending on the severity of the deficiencies and the known reliability and attitude of the facility, the CSO may either conduct a special inspection to determine whether the deficiencies have been corrected or accept management's written statement that the corrective action has been accomplished subject to verification at the next inspection.

Part 2. UNSATISFACTORY INSPECTIONS

4-200 Application. This part establishes procedures to be followed in instances of unsatisfactory security inspections, or whenever there is an immediate danger of classified information being compromised.

4-201 Procedures.

a. . If a CSO determines that there is an immediate danger of classified information being compromised 3/ or if a security inspection conducted under the provisions of part 1 of this section results in an overall facility security evaluation of "unsatisfactory," the CSO shall notify immediately the Regional Director and the Director, DIS, ATTN: Deputy Director (Industrial Security), of all pertinent facts. That office shall also be kept informed of all subsequent developments. In addition, the actions described below shall be taken.

(1) The Regional Director shall notify the contractor that the existing deficiencies shall be corrected within the period of time prescribed (not to exceed 30 days) and of the possible consequences if satisfactory action is not taken. Include in the letter to the contractor a statement that the contracting activities have been notified of the existing conditions.

(2) Within 3 days from the completion of the inspection, notify by electrical message the contracting officer(s) concerned of the nature and scope of the deficier.ties, the specific contracts which are

---

3/ In every case where there is immediate danger of classified information being compromised, require the contractor to take immediate measures to safeguard the classified information. If the contractor refuses or is unable to take immediate corrective action, the CSO shall recover, or arrange with the contracting officer(s) concerned-, for the recovery of the classified information.

affected, the action taken by the contractor to remove the danger of compromise, if any, and the contractor's plan to correct the deficiencies and the scheduled date for completion. (Actions by the contracting officer(s) are not required at this time.)

(3) Conduct reinspection immediately following the end of the period prescribed for correction of the deficiencies to determine whether necessary corrective action has been taken or whether an additional period of time should be granted in which to complete the corrective action. If the CSO is satisfied that management has taken adequate action to correct the deficiencies, electrical message notification of the "satisfactory" evaluation will be sent to the same addressees who received--the notification as to the "unsatisfactory" evaluation.

b. If there is no immediate danger of compromise of classified information but the contractor nevertheless has failed to correct the deficiencies within the allotted period (or any extension thereof), the Director of Industrial Security shall notify the contracting officer(s) concerned, each contractor having a classified subcontract in the facility, and each contracting UA 4/ that the release of additional classified information to the facility should be withheld, except for information necessary to the completion of essential contracts. In addition, such notification should also state that the facility is considered ineligible to receive requests for proposals or invitations to bid on or for the award of new classified contracts. A copy of this notice shall be furnished the DUSD(P), ATTN: DSP&P through the Director, DIS. The contracting UA shall determine whether to terminate existing classified prime contracts or whether the overall defense interest requires their completion.

4/ As appropriate, notices to contracting UA's specified in this paragraph shall be addressed as follows:

Assistant Chief of Staff for Intelligence, USA, ATTN: DAMIDOS, Washington, D.C. 20310
Chief of Naval Operations, Director of Naval Intelligence, ATTN: 009D, Washington, D.C. 20350
Director of Security Police, USAF, ATTN: IGSPA, Washington, D.C. 20335
Director of Security, NASA, ATTN: Code LZ, Washington, D.C. 20546
Chief, Security & Investigations Division, Small Business Administration, Washington, D.C. 20416
Security Officer, National Science Foundation, Washington, D.C. 20550
Director of Investigations and Security, Department of Transportation, Washington, D.C. 20590
Security Office, Department of the Treasury, Washington, D.C. 20220
Chief, Division of Enforcement and Security Management, Department of Interior, Washington, D.C. 20240
Department Security Officer, Department of Agriculture, Washington, D.C. 20250
Chief, Physical Security Division, United States Information Agency, Washington, D.C. 20547

When classified subcontracts are involved the ACO will make this determination after appropriate coordination, and advise the concerned prime and subcontractor if the classified subcontract is to be terminated. If, on . completion of existing contracts, the security deficiencies have not been corrected, take the action prescribed in paragraph c below, unless it has been previously taken.

c. When a contractor persistently fails or refuses to discharge his or her obligations under the "Department of Defense Security Agreement" to protect classified information, the CSO shall recommend to the Director, DIS, ATTN : Deputy Director (Industrial Security), through the Regional Director, the revocation of the FCL. That office shall make all reasonable efforts to secure the compliance of the contractor. If these efforts are not successful, the Director, DIS, after consultation with the concerned contracting officer(s) and contracting UA's, shall authorize the CSO through the Regional Director to revoke the facility clearance (see paragraph 2-121). Copies of such authorizations will be furnished to DSP&P.

d. When an authorization to revoke a FCL is received the CSO shall:

(1) immediately notify each contractor having a classified subcontract in the facility that the subcontractor's FCL is being revoked and that he or she, as a prime contractor, shall without delay submit a listing of existing classified subcontracts in the facility to the contracting officer(s) concerned, requesting instructions with respect thereto;

4/(Continued)
Director of Investigations and Security; Department of Commerce, Room 5004, Main Commerce Building, Washington, D.C. 20230
Director of Investigations, General Services Administration, Washington, D.C. 20230
Director of Security, AlTN: SY/DO, Department of State, State Department Bldg., Washington, D.C. 20230
Director, Investigations and Security, Office of the Assistant Secretary for Administration, Department of Labor, Washington, D.C. 20210
Director, Security and Inspections Staff, Environmental Protection Agency, Washington, D.C 20460
Director, Office of Safeguards & Security, U.S. Department of Energy, Washington, D.C. 20545
Director, Security and Administrative Programs Staff, Office of Management and Finance, Department of Justice, Washington, D.C. 20530
Security Officer, U.S. Arms Control and Disarmament Agency, Washington, D.C. 20451
Security Officer, Federal EmergencyM anagement Agency, 1725 I"Street, NW, Washington, D.C. 20472
Director, Office of Security and Safety, U.S. General Accounting Office, Washington, D.C. 20548
Chief of Security, Board of Governors, Federal Reserve System, 20th end C Streets, N.W., Washington, D.C. 20551

(2) recover, or arrange with the contracting officers(s) concerned for the recovery of all classified information; and

(3) after all classified information has been recovered:

(a) terminate the contractor's DD Form 441 in accordance with section IV of the agreement,

"(b) withdraw the DIS FL 381-R,

(c) forward a DIS Form 553 to DISCO annotated to indicate revocation of the FCL on grounds pertaining solely to the physical elements of security, and

(d) forward a copy of DIS Form 553 reflecting the "revocation action to the DTIC.

4-202 Unsatisfactory Evaluation of a Commercial Carrier.

a. Whenever the inspection of a carrier terminal results in an unsatisfactory evaluation, the CSO, in coordination with the CSO of the HOF, will make every effort to have immediate corrective action taken. A copy of the inspection report and related correspondence will be furnished MTMC for "information only" at this point in time.

b. If immediate and effective corrective action cannot be obtained, the CSO, in coordination with the CSO of the HOF, will recommend to the Director, DIS, ATTN: Deputy Director (Industrial Security) through the Regional Director that the FCL of the terminal or the authorization for the carrier's organization to transport SECRET materials be revoked under the provisions of paragraph 2-121. Simultaneously MTMC will be requested to suspend further use of the carrier's terminal involved in shipments of SECRET materials pending decision by the Director, DIS. However, SECRET shipments already in transit may continue to be transported by the carrier to consignee.

c. Every reasonable effort will be made to have the HOF of the carrier effect required corrective action. If unsuccessful, the Director, DIS may authorize the CSO to revoke the FCL or the carrier's overall authorization to transport SECRET materials and advise the DUSD(P), ATTN: DSP&P of the action. On receipt of such notice the CSO will take the directed action and notify MTMC that the carrier (or a specific terminal) is no longer authorized to handle controlled shipments of SECRET materials.

d. If, prior to revocation, compliance with security requirements is obtained, the CSO will notify MTMC.

Part 3. "CLOSE-OUT" INSPECTIONS

4-300 A "close-out" inspection, that is, a formal DD Form 696 inspection, shall be accomplished immediately prior to action to administratively terminate a FCL or revoke a FCL. When conducting a "close-out" inspection, all areas and containers authorized for the storage of classified material shall be checked, including a spot check of other containers and areas where

classified material could reasonably be expected to be improperly stored or maintained, the latter of which shall be conducted only with the full knowledge and consent of management. Should management object to the foregoing spot-check of their non-approved areas or repositories, this fact and purported rationale shall be indicated under "Remarks" on the DD Form 696. In addition, the "Remarks" section of the DD Form 696 shall contain statements regarding: (i) the location where accountability records, records of receipt and dispatch, debriefing statements, document receipts, visitor records, destruction certificates, and so on, will be retained for the prescribed period of time, (ii) that the facility is not performing on any classified contracts, subcontracts, or proposal efforts, and (iii) * action taken to ensure that all debriefings have been (or will be) accomplished and that outstanding classified visit authorizations have been canceled. The "close-out" inspection shall be a complete inspection * effort, to include a listing of all deficiencies observed, inasmuch as management may justify retention of the FCL prior to completion of the termination action. A refusal by management to permit the industrial security representative to conduct a spot check of non-approved areas or repositories is not in itself significant. However, If the CSO has reason to believe that classified material remains in the facility in non-approved areas or repositories, termination of the FCL shall be held in abeyance and the matter referred to the Director, DIS, Al'TN: Deputy Director (Industrial Security).